



Office de la propriété
Intellectuelle
du Canada

Un organisme
d'Industrie Canada

Canadian
Intellectual Property
Office

An Agency of
Industry Canada

COPY OF PAPERS
ORIGINALLY FILED




*Bureau canadien
des brevets*
Certification

*Canadian Patent
Office*
Certification

La présente atteste que les documents
ci-joints, dont la liste est ci-dessous,
sont des copies authentiques des docu-
ments déposés au Bureau des brevets.

This is to certify that the documents
attached hereto and identified below are
true copies of the documents on file in
the Patent Office.

Specification and Drawings, as originally filed, in Application for Patent Serial No:
2,332,255, on January 24, 2001, by JAMES A. ... for "Automated Mortgage Fraud
Detection System and Method".


Agent certificateur/Certifying Officer

January 7, 2002

Date

Canada

(CIPO 68)
01-12-00

OPIC  CIPO

ABSTRACT

An automated system and method for detection of mortgage fraud is disclosed. An automated system screens mortgage loan application queries and compares the query data against data within a property database. The comparison indicates whether possible fraud indicators are present in the query data. Post-transaction is further analysed to determine whether possible fraudulent transactions have taken place.

AUTOMATED MORTGAGE FRAUD DETECTION SYSTEM AND METHOD

FIELD OF THE INVENTION

The invention relates generally to fraud detection systems and more particularly to the automated detection of fraud related to property mortgages.

BACKGROUND OF THE INVENTION

Mortgage fraud is a clearly undesirable but pervasive problem in the property market. Such fraud typically results in the granting of loan funds secured by a mortgage where the normal process of lending due diligence is circumvented through individual deception or fraudulent collusion between parties in the lending process. While mortgage fraud occurs in a small percentage of the overall number of transactions in the industry, the losses associated with such fraud amount to consequential losses to financial institutions. Fraudulent activity tends to have certain repetitive patterns associated with it and typically leaves behind trails comprising certain types of data.

Mortgage fraud takes many forms. "Self-serving" fraud may be defined as fraud perpetrated by single potential borrowers in order to secure loans, which they intend to pay back. "Malicious" frauds may be defined as those where the clear goal is to take the money without any intention of repayment. Even worse are organized schemes where a series of loans based on fraud is the goal. All these types may be characterized by certain repetitive patterns.

The problem of mortgage fraud has not been solved. It is known in the art that lender representative training and compliance with stated lending policies help to alleviate the

problem. Property searches can be conducted regarding specific properties to determine transaction histories related to specified properties.

However, mortgage fraud is generally recognized as an industry-wide problem and attempts by single institutions have failed to address the problem. Lender representative training and due diligence cannot properly assess information related to properties and borrowers where multiple lending institutions are involved in multiple transactions. Property searches cannot provide information related to queries made in relation to properties that do not form the basis of a registered transaction. Furthermore, property searches are property-specific and do not provide information about communities or cities. As such, they cannot provide comparative data with which to use in fraud detection. In addition, these methods are ineffective when the person charged with conducting the due diligence or property search colludes with the fraudulent activity.

Therefore, it is desirable to have a system and method for the automatic detection of mortgage fraud where transaction-related queries may be compared with data within a database and it may be determined whether the query data triggers an indication of fraudulent activity.

SUMMARY OF THE INVENTION

The invention is directed to the automated detection of mortgage fraud. The invention is an automated system that screens mortgage loan application queries and compares the query data against a database of property and sales data. The database acts as a current audit of industry activity involving loans where properties are used as collateral. A set of automated fraud detection indicators ("red flags") is provided which is intended to be used within the lending process to increase diligence in certain situations. Red flags are raised when certain patterns are detected in supporting data that indicate increased risk.

Embodiments of the invention have several advantages. For example, queries regarding potential mortgage transactions are in fact sources of data that may be stored on a database and then retrieved and analysed in subsequent queries. The system guarantees loan criteria compliance within financial institutions where the system is implemented. Red flags returned may be based on database data from many financial institutions, other related institutions, and a broad scope of relevant comparative property transaction and query data. The method and system may be employed automatically in all mortgage transaction queries thus eliminating the potential for fraud by financial institution representatives. Lower overall portfolio risk is achieved by focusing manual due diligence on those cases that are not safe enough to pass automated process.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will further be described with reference to the attached drawings showing an embodiment thereof:

Figure 1 is a schematic diagram illustrating components within a system for automated mortgage fraud detection in accordance with an embodiment of the present invention.

Figure 2 is a flowchart illustrating an automated mortgage fraud detection method in accordance with an embodiment of the present invention.

Figure 3 is a flowchart illustrating an automated mortgage fraud detection method related to post-transaction data in accordance with another embodiment of the present invention.

Figure 4 is a screen illustration of property data indicating a condition for a red flag as defined by financial institution parameters.

Similar references are used in different figures to denote similar components.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

An automated mortgage fraud detection system and method is disclosed. The invention automatically flags situations indicating potential fraud before the loan is funded allowing increased diligence where it may be warranted. The invention further allows an audit to be conducted of property transactions that have taken place among multiple properties and then compares property transaction data with data from a database to determine if potential fraud indicators are present. In a preferred embodiment, the actual interface between the financial institution ("FI") and the system and database is through a direct electronic data link from the FI's lending system, eliminating any possibility that the fraud detection step can be skipped.

Each FI may implement its own procedures to deal with any red flags that occur as part of its normal lending process. The invention provides for customized messages or instructions, scripted by the FI to the loan officer to indicate how to proceed with a red flagged situation.

Types of Fraud in Mortgage Lending

Fraud can take many forms in the lending process. Probably the most common are "self-serving" activities in which the object is to qualify for a loan by supplying misleading information. In most of these cases, the applicant's intent is to secure the loan, and repay it. Unfortunately, in some instances, the loan does not get repaid and the FI must then attempt to realize on its security. If the property was over valued at the time the loan was given, the bank will be under-secured and will be left with a shortfall when the property is sold.

There are more serious "malicious" frauds, where the object is to take the money and run. Even worse is to take the money and do it again, or systematically engage in a series of fraudulent loans.

In the case of these more serious fraud schemes there tend to be some general trends. There is typically collusion between some parties in the process. These tend to involve property sales, rather than refinances. They tend to happen with new clients, or alternatively, fraud tends to be less of a factor when dealing with long term clients. Repetitive behavior is also present with fraudulent activities involving the same properties, participants and names. Frauds generally do not happen as much with owner occupied properties.

Sophisticated frauds schemes also tend to be perpetrated across many different lending institutions, making it difficult for any single organization to deal successfully with the problem. It is an industry concern.

In many cases, these frauds are actualized through the vehicle of "flipping" properties between parties, where the value of the property artificially rises dramatically. In some cases, the property will change hands on the same day (or in a relatively short time) at markedly different values, with loans made based on inflated values. These inflated values may be substantiated through a variety of methods. In many cases, there may be separate transactions involving multiple lenders.

The invention detects flips by searching for suggestive patterns. Two separate data streams may be reviewed in the search: (a) the incoming query which includes data relating to intended transactions; and (b) post-transaction data.

Regular Followup Audit

Due to the nature of the data flow into the database in a preferred embodiment of the invention it may be difficult to flag all flips instantaneously. To deal with this, a followup audit may be instituted. For example, on a regular basis, (generally monthly), as sales data becomes available, a special processing query may be directed to all of the latest posted sales to determine if, based on the new information, there are any properties which have a new or changed "flipped" status. The list of any properties newly flagged as potential flips may be made available to FIs and may be processed against their portfolios.

This process is intended to provide a regular audit of potential fraudulent situations and to trigger subsequent investigative action by each FI. While these loans may already be funded, it is intended to flag potentially high-risk situations as soon as possible based on the availability of the data trails, and to eliminate repetitive schemes.

Red Flags

Red flags may be based on an analysis of several patterns consistent with known cases of fraudulent activity. They may also be based on detecting similar patterns in the data associated with a specific property in a specific neighborhood. Red flags are intended to highlight specific situations allowing lenders to apply increased due diligence where it is warranted.

It must be stated that any pattern of data can occur in legitimate circumstances, and that red flags cannot be taken to indicate that fraud actually exists. In addition, the absence of any red flags cannot guarantee that any transaction is completely legitimate. Finally, the necessary data is not always available. Nevertheless, the very nature of these red flags, derived out of a database, offers a unique and valuable additional tool for FIs.

What follows are examples of the types of red flags, or fraud indicators, that may be detected by embodiments of the invention:

Unusual Market Activity

It is common to receive multiple queries for the same property, many times coming from different lenders. Multiple queries by themselves are not a concern. However, if the declared value on multiple queries on the same property are significantly different, a red flag may be generated.

Flip Detected

This red flag indicates that a pattern associated with a property flip has been determined in the sales transactions associated with the subject property. In general, this means that two transactions of the same property have been registered, within a given period, where the value of the property changed significantly. As an example, a flip could be defined as a \$30,000 difference between two sales within a six-month period.

There are many situations that satisfy the above criteria which would not be considered part of any fraudulent activity. For example, virtually every newly built property sold to

first time buyers, from the original builder, could be defined as a flip under the above definition. These can be identified separately if desired, but will typically not be red flagged as a flip. For the purposes of defining these builder transactions, the seller name must match to a list of known builders, and the transactions must be the first on record for the subject property. The flip definition may be customized by a FL. There are several other criteria that have been identified which are used to eliminate "false positives".

Flip Percentage

This red flag indicates there is an unusually high proportion of properties in the neighborhood with a history of flips.

Rental Property

This flag indicates there is some history of this property being rented out. In a preferred embodiment, this flag will only be shown in those circumstances where another red flag is present.

Seller Name doesn't match registered Owner Name

This flag indicates the name of the seller does not match any of the names of the registered property owner.

Buyer or Seller name matches Neighborhood "Common" name.

This flag indicates that the buyer or seller appears unusually frequently as a participant in sales transactions within this area. The area considered may be a municipality and a

separate list of "common" names may be maintained for each area, based on the transactions on file.

The following flags are available only if a reavs system valuation, described below, is also run as part of the same transaction.

Declared Value Inconsistently High

Reavs system technology is aimed at providing consistent property valuations which can be safely used in the lending process. As part of its valuation technology, the reavs system measures the consistency of each sale on record against sales of like properties within the neighborhood. This consistency check is one of several filters used to determine which of the many sales on record will be used for valuation purposes. Any inconsistent sales may not be used for valuation purposes.

It is to be expected that many of the declared property values will be greater than reavs system values, and this will not in itself be taken as a potential problem. However, if a reavs system valuation is also run as part of the transaction, and the declared value is inconsistently high (i.e. it is statistically aberrant), then the transaction may be red flagged.

High Inconsistent Sale

This flag indicates there has been a registered sale of this property which is inconsistently higher than expected (i.e. statistically aberrant), based on reavs system consistency limit for this property. The criteria used here is the same as described earlier for the declared value.

Multiple queries indicate unusual market activity

Perhaps the best chance of detecting a potential fraud before funding comes from analysis of any other transactions associated with the same property. There are hundreds of examples of multiple queries on the same property, most of which would be naturally expected to occur out of the normal lending process. However, consider this pair of transactions, on the same property:

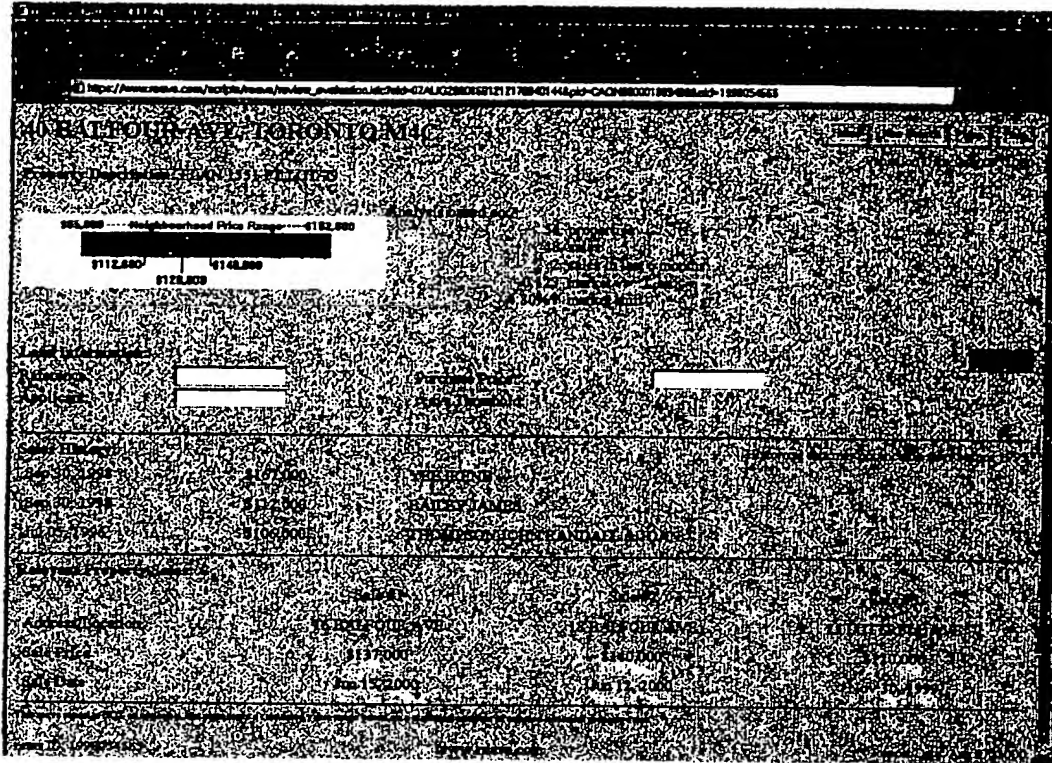
Date	Declared Value	Requested Loan \$	Lender	Reavs Value
7-Jan-00	\$142,000	\$106,500	Lender A	\$140,700
16-Feb-00	\$245,000	\$183,750	Lender B	\$141,200

The first query is unremarkable, and the declared value is certainly reasonable against the reavs' calculated value. Within 6 weeks, the value of this property has apparently increased over \$100,000, and the loan requested on the second query is greater than the previously declared value of the property. While this situation could be legitimate, a flag signalling "Unusual Market Activity" would be raised automatically on the second query related to the loan application.

Flips detected from registered sale transactions

For illustrative purposes in identifying flips, consider the example shown below. Note that the definition of a "flip" may be customized by or for each separate FI. In the

example, the property was "flipped" on the 30th of September, 1998 when it increased in value by \$55,000 on the same day.



The invention may be incorporated into other data analysis tools such as the Reavs system. The Reavs system validates residential property values. Once all other credit checks and lending criteria have been satisfied, it acts as a filter, to determine whether

this particular application can be approved by reavs alone, or if additional scrutiny of the property is required. The basic process of the reavs system is as follows:

- The address is supplied to the reavs system, and it returns its calculated valuation and other relevant information for that property.
- The loan type, property value (purchase price or declared value), and loan amount are entered.
- The reavs system returns a Yes or No response, indicating whether this particular transaction can be approved immediately, using criteria approved by the lending institution.

If the transaction is not approved through the reavs system, it does not mean that the application is denied. It simply means that it is not safe enough to be approved through the reavs system alone, and that other scrutiny, such as a traditional appraisal, may be required.

Common name in a database

In repetitive cases repeated flips may occur between the same parties in the same general area and the property sales will occur using the names of fictitious or unknowing people. In many cases, the same name will be used repeatedly. Many times, the actual name of the seller will not be the same as the registered owner of the property.

Each registered sale in the invention's database generally includes both a buyer and seller name, although these names are not always available. If so, the invention

maintains a database of the number of times that the same name is used in a transaction, as buyer or seller, in each neighborhood. All subsequent transactions are to be checked against this database.

Referring to Figure 1, there is illustrated a block diagram of an operating environment in accordance with an embodiment of the present invention comprising a potential fraud detector/ red flag generator 10 connected by a series of data links 22, 24, 26, 28 and 30 to a number of institutions. Such institutions include financial institutions 12, 14 and 16, as well as other institutions 18 and 20. Financial institutions may include banks or other mortgage lenders. Other institutions may include credit bureaus and other credit checking facilities. A property database 32 is connected to the potential fraud detector / red flag generator 10 and stores data relating to queries regarding properties as well as transactions regarding properties.

Referring to Figure 2, there is illustrated a flow chart in accordance with an embodiment of the present invention comprising the operation of an automatic fraud detection method. In a step 50, a financial institution (FI) transmits a query including property data to the fraud detector / red flag generator 10. In a step 52, the FI query data is received by the potential fraud detector 10. In a step 54, the FI query data is stored in a database 32. In a step 56, the FI query data is compared with data within the database 32, and the potential fraud detector / red flag generator determines whether a red flag should be generated 58. If so, the red flag including other data is returned to the FI 60, and this may end the transaction 62. If no red flag is generated, the appropriate response is returned to the FI 64, and this may end the transaction 66.

Referring to Figure 3, there is illustrated a flow chart in accordance with an embodiment of the present invention comprising the generation of an automatic mortgage fraud detection method. In a first step 80, a FI submits a query for information regarding the transaction history of a property or a number of properties. In a step 82, this query data is received by the potential fraud detector / red flag generator 10. In a step 84, the FI query data is compared with data contained within a database 32, and the red flag generator determines 86 whether a red flag ought to be generated based on the comparison of this data. If so, the red flag, including other data, is returned to the FI 88, and this may conclude the transaction 90. If no red flag is generated, 92, the appropriate data is returned to the FI and this may conclude that transaction 94.

Referring to Figure 4, there is illustrated a diagram in accordance with an embodiment of the present invention showing information indicating that the subject property was "flipped" on the 30th of September, 1998. On this day, the property is shown as increasing in value by \$55,000.00. It should be noted that the definition of a "flip" may be customized by or for each separate FI.

The many features and advantages of the invention are apparent from the detailed specification, and thus, it is intended by the appended claim to cover all such features and advantages of the invention which fall within the true spirit and scope of the invention. Further, since numerous modifications and variations will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation illustrated and described, and accordingly, all suitable modifications and equivalents may be resorted to falling within the scope of the invention.

What is claimed is:

1. An automated fraud detection system for operation via a data link comprising:
 - means for receiving through said data link a query comprising first data,
 - means for comparing said first data with second data from a database,
 - means for determining, based on said comparison, whether said first data indicates potential fraud.

2. An automated fraud detection method comprising the steps of:
 - receiving through a data link a query comprising first data,
 - comparing said first data with second data from a database,
 - determining, based on said comparison, whether said first data indicates potential fraud.

3. An automated fraud detection system comprising:
 - means for reviewing first data,
 - means for comparing said first data with data from a database,
 - means for determining, based on said comparison, whether said first data indicates potential fraud.

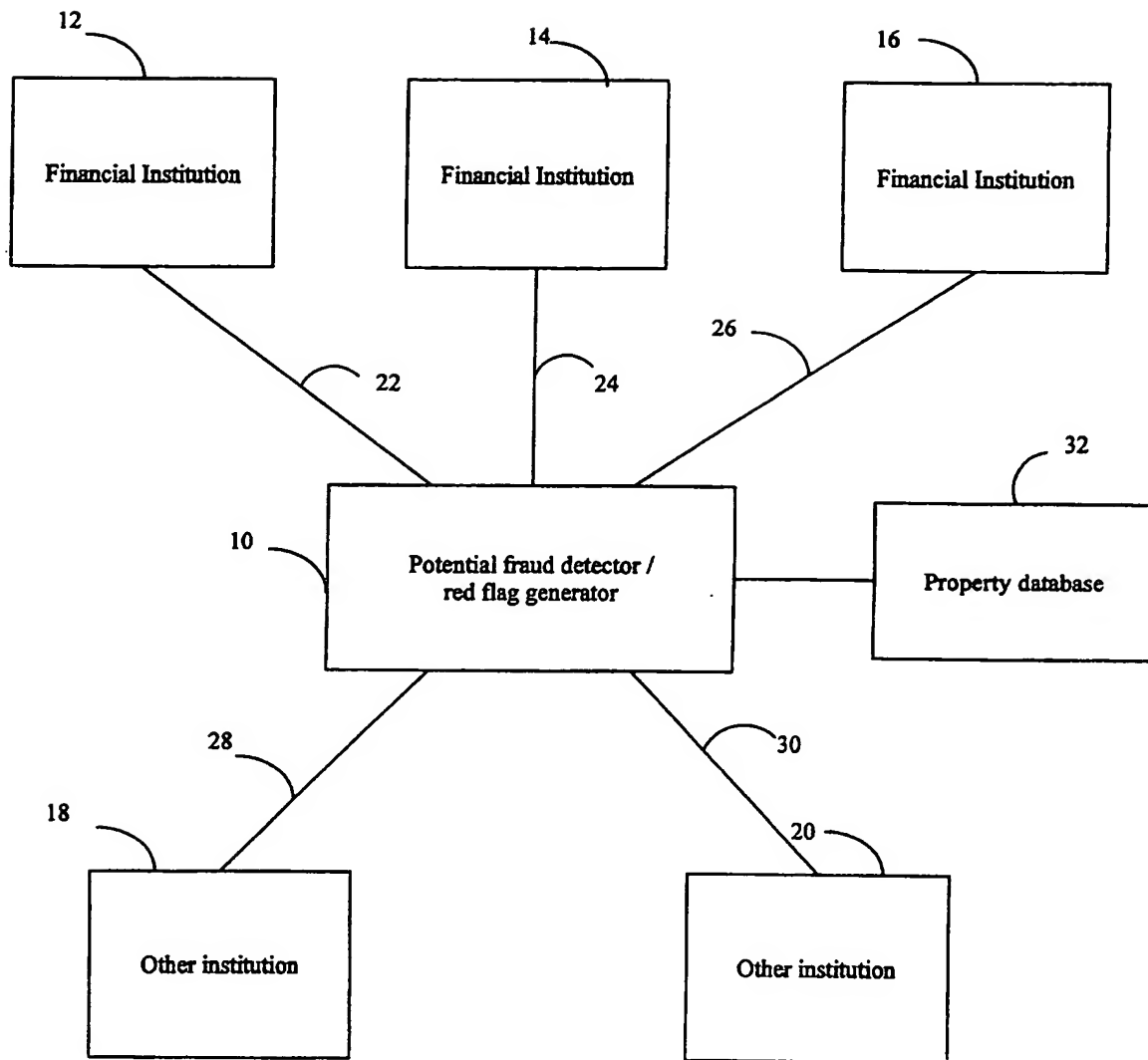
**FIG. 1**

FIG. 2

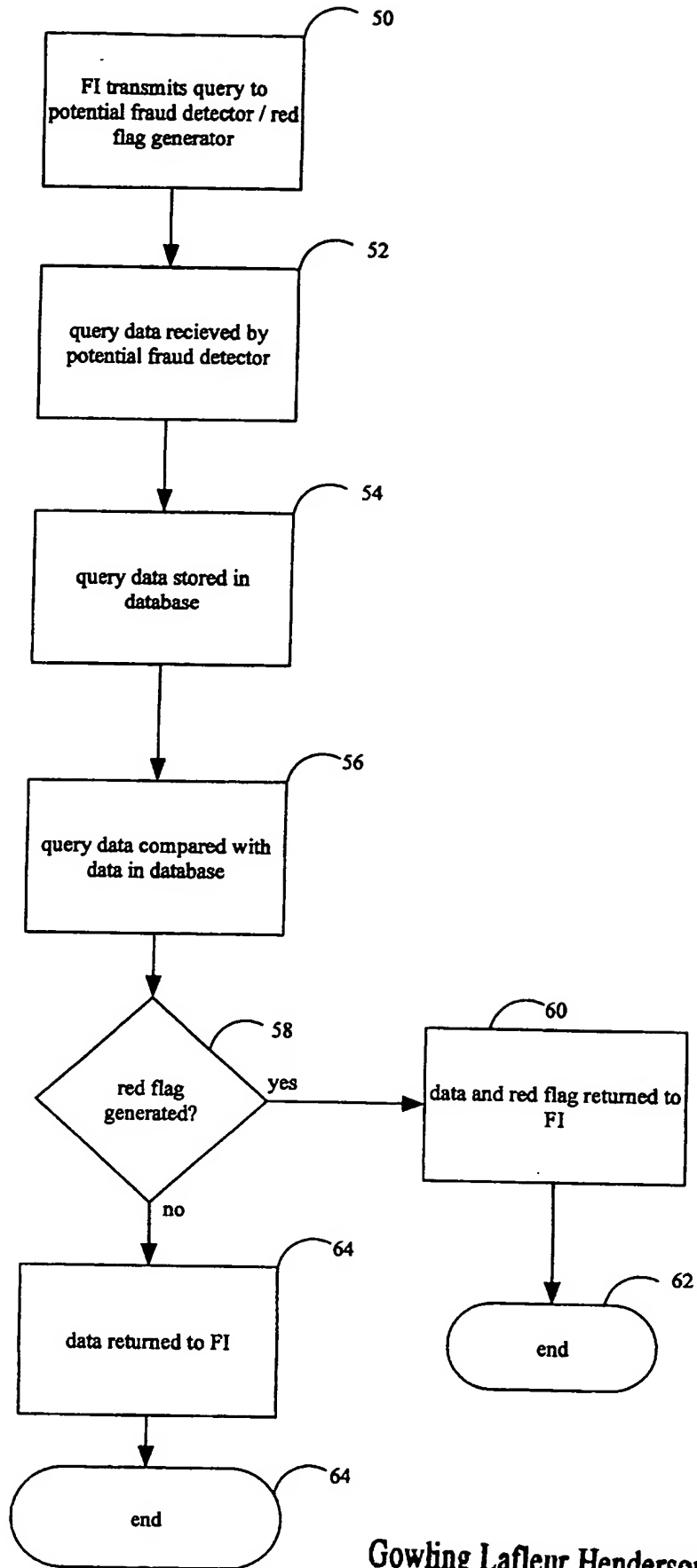
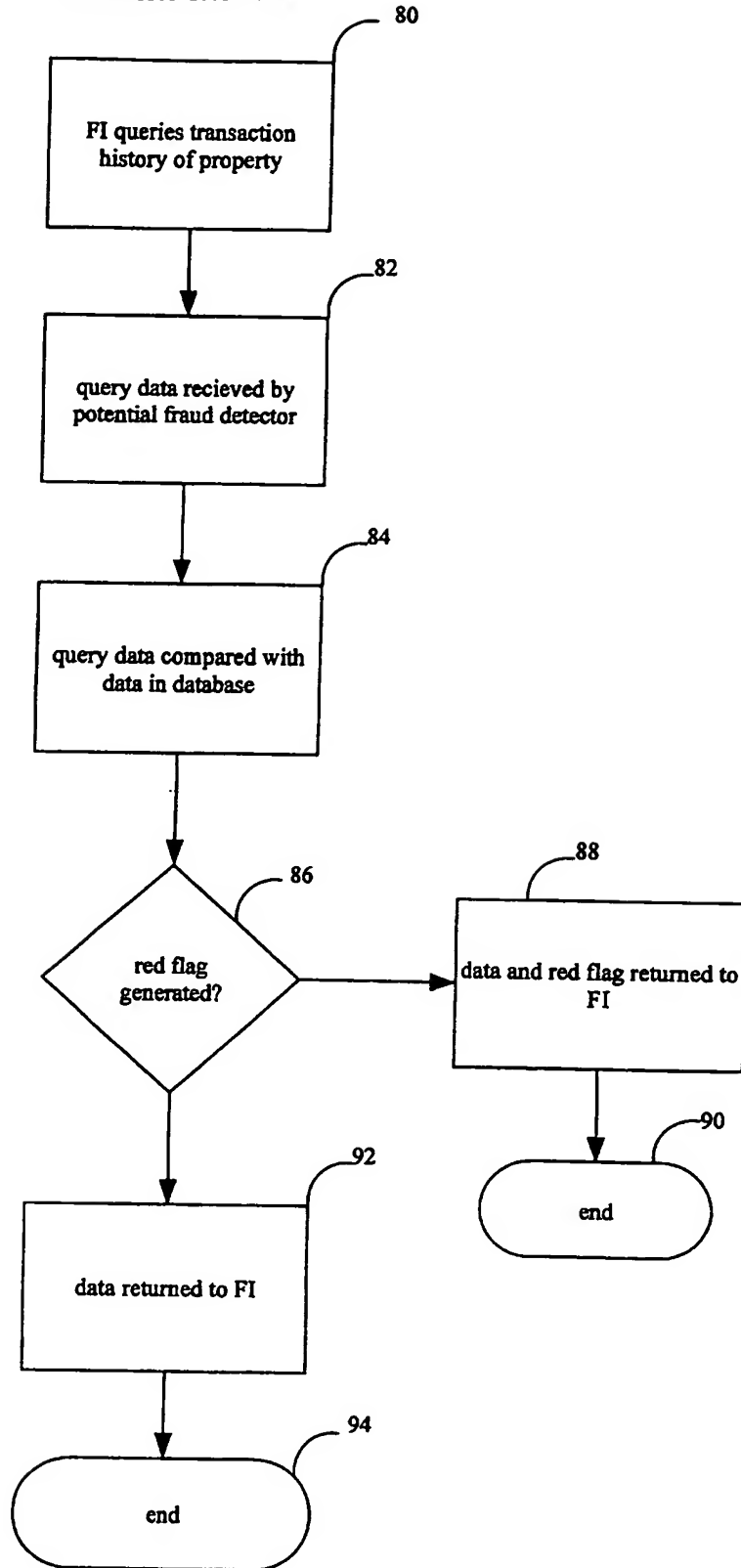


FIG. 3



BEST AVAILABLE COPY

FIG. 4

40 BALFOUR AVE, TORONTO M4C

Property Description: PLAN 1331 PT LOT 79

Valuation Date: Aug 07, 2000

Analysis based on:

54 properties
48 sales
2 sales in last 6 months
0.123 market variation
4.30% market shift

Neighborhood Price Range: \$112,000 - \$122,000

Loan Information:

Reference: _____ Purchase Price: _____ LTV: _____

Applicant: _____

Sales History:

Date	Price	Buyer
Sep 30, 1998	\$167,000	YEE, IRENE
Sep 30, 1998	\$112,000	BAILEY, JAMES
Jul 05, 1996	\$106,000	THOMPSON, JOHN RANDALL & JOAN

Historical data may not include sales before 1993.

Relevant Property Sales:

	Sale #1	Sale #2	Sale #3
Address/Location	16 BALFOUR AVE	18 BALFOUR AVE	23 LUTTRELL AVE
Sale Price	\$137,000	\$140,000	\$120,000
Sale Date	Jun 15, 2000	Jun 12, 2000	Nov 30, 1999

This report is NOT an appraisal, but represents a calculated value range based on a statistical analysis of selected historical property sales.

Report ID: 1998054565

www.revel.com

Report Date: Aug 07, 2000

Gowling Lafleur Henderson LLP